



UNITED STATES MARINE CORPS
U.S. MARINE CORPS FORCES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

MARCENTO 5510

SecMgr

AUG 25 2006

U. S. MARINE CORPS FORCES, CENTRAL COMMAND ORDER 5510

From: Commander, U. S. Marine Corps Forces, Central Command
To: Distribution List

Subj: U.S. MARINE CORPS FORCES CENTRAL COMMAND (MARCENT) COMMON
INFORMATION TECHNOLOGY (IT) WIRELESS SECURITY AND
REMOVABLE SECONDARY STORAGE MEDIA DEVICE ORDER

Ref: (a) DODD 8100.2
(b) USCENTCOM MSG DTG 221738Z AUG 03

1. Situation. To establish a U. S. Marine Corps Forces, Central Command (MARCENT) order per the guidance contained in reference (a). "Cellular/PCS and/or other RF [Radio Frequency] or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA [Designated Approving Authority] in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

2. Mission. To establish policy governing the use of wireless communications devices and removable secondary storage media by personnel within MARCENT headquarters facilities in order to safeguard classified materials and information.

3. Execution

a. Commander's Intent. Due to operational need, command issued 'Blackberrys' and other command issued phones are authorized to remain in an active status once the device's infrared (IR) capability is disabled utilizing 'Metallic Aluminum or Copper Foil' tape. The tape shall extend beyond the IR port to ensure no diffracted light is able to escape or enter around the fringes of the tape. The MARCENT G-6 will apply the appropriate tape to all command Blackberry's.

b. Subordinate Element Missions. Ensure that all personnel are aware of reference (b), which prohibits the use or connection of personally owned removable secondary storage media (e.g. USB thumb drives) with any government-computing device due to the inherent security risk that they pose. Only government-procured removable

secondary storage media devices issued by the Assistant Chief of Staff, G-6 are authorized for use on NIPRNET or other unclassified and classified computer systems.

c. Coordinating Instructions.

- (1) All Cellular/PCS and/or other RF [Radio Frequency] or Infrared (IR) wireless devices and personnel electronic devices will be turned off prior to entering the facilities.
- (2) Personnel desiring to use personal wireless devices will exit the building.

4. Administration and Logistics

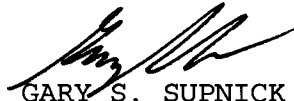
a. Duty and Command Security Personnel are authorized to confiscate wireless/removable storage devices from individuals that disregard this guidance; the devices will be turned over to the Chief of Staff for disposition. Repeated violations that jeopardize the security of MARCENT facilities may result in administrative or punitive action.

b. This policy does not apply to the MARCENT Sensitive Compartmented Information Facility (SCIF). Regulations that govern Common IT Wireless Security in the SCIF fall under the purview of the Director of Central Intelligence Directive (DCID) rules.

5. Command and Signal

a. Command. This policy applies to all individuals and units that use MARCENT spaces.

b. Signal. This order effective date signed.


GARY S. SUPNICK
Chief of Staff

Distribution: A